

Position Description



Cyber Security Analyst

Division	Corporate Services
Team	Business Technology Services
Location	Adelaide
Classification	ONRSR Enterprise Agreement - Specialist 1
Reports to	Manager, Information Security
Direct Reports	Nil
Key Relationships	Internal: Director Governance & Risk, Safety & Regulatory Insights team, Regulatory & Data Product Development team, Manager Service Delivery & Operations, IT Architecture & Project Lead, Business Unit leads External: IT Vendors and Service Providers and External Auditors

About ONRSR	The Office of the National Rail Safety Regulator (ONRSR) plays an integral role in keeping Australians safe across the nation's vast and varied rail networks. Headquartered in Adelaide, and with offices around the country, ONRSR is an independent regulatory authority that encourages safe rail operations, enforces national compliance with the <i>Rail Safety National Law</i>, and promotes and improves rail safety throughout Australia.
Our People and Our Culture	At ONRSR we aim to enhance and promote rail safety nationally through effective risk-based regulation. To achieve that, we need people with the vision to contribute to the safety of Australia's railways – people who are professional and motivated by the opportunity to improve rail safety and by the benefits this delivers to the Australian community. We recognise that a diverse workforce strengthens our capability by bringing together different perspectives, experiences, and skills. We are committed to creating an inclusive environment that enables all staff members to contribute fully. By fostering this culture, we support collaboration, drive innovation, enhance decision-making, and elevate our overall organisational performance

	Our culture reflects our values of Integrity, Respect, Independence, Diligence and Excellence in the way we work, lead and engage with others. Our Culture Blueprint guides us to create a respectful, inclusive and equitable workplace where diversity is embraced, and every individual can contribute, grow, and thrive. Every role plays a part in shaping this culture.
Our Purpose	Safe railways for Australia
Your impact and contribution	The Cyber Security Analyst plays a key role in securing systems, applications, infrastructure and AI enabled technologies. Your work will directly influence the safety, trustworthiness and resilience of our software ecosystem, ensuring that security is embedded through the development lifecycle and beyond. Your technical expertise will enable you to analyse and secure networks and cloud environments ensuring they are resilient against evolving cyber security threats. By implementing and managing security controls, monitoring network traffic and supporting incident response efforts you will help maintain operational continuity and protect sensitive data from compromise. You will work closely with the cyber security and network managed service providers to ensure our environment is secure and monitored. You will collaborate with the business to foster a positive culture of security understanding and awareness. A key focus for this role is managing security risks, supporting the development and maintenance of the cybersecurity strategy and managing identity and endpoint security policies alongside the cyber security managed service provider. This role will support secure application workflows as well as threat detection and incident response and business continuity and disaster recovery plans.
Your Responsibilities	Applying your passion for unique cyber security changes and your enthusiasm for securing risk vectors you will: • Support the effective management of end point detection response (EDR) and Security Event Information Management (SEIM) working closely with IT Vendors and Service Providers. • Support the effective management of End Point Security aligning with Essential8 maturity 2. • Provide effective administration of identity and access management systems. • Coordinate external penetration testing, vulnerability management and threat awareness activities in partnership with external IT vendors, ensuring secure development practices and AI controls and reporting. • Contribute to the identification of Cyber security risks under the Enterprise Risk Management framework and actively manage assigned risks for closure. • Provide oversight and monitoring of security controls, regularly assessing and evaluating our security posture to provide recommendations to the Information Security Manager on enhancements that could be made.

- Manage ONRSR's threat and vulnerability framework controls, oversee Endpoint management using Intune, Action1 and Airlock, and manage physical security, including building access and monitoring systems.
- Contribute to the development and implementation of security and compliance strategies to protect ONRSR's information assets and ensure adherence to regulatory requirements.
- Monitor, audit and ensure that all IT vendors, data partners and other parties comply with ONRSR cyber security standards and policy.
- Manage and monitor all device policies in Intune and ensure they are as consistent as possible with Essential 8 Level 2 compliance.
- In collaboration with the Manager, Service Delivery & IT Operations, develop and monitor BYOD policy and SoE to ensure that allowed use cases are consistent with policy.
- Support the development and documentation of cyber security and infrastructure related IT policies, procedures and work instructions.
- Establish and maintain an appropriate whitelist of applications, IP addresses and email domains/addresses.
- Monitor Action1 for patching requirements, and for large patches, ensure that patches are tested.
- Establish and document procedures, in collaboration with the BTS leadership team, to conduct software development assessments and identify when PEN testing should be undertaken.
- In partnership with external vendors establish a program to monitor CoPilot and AI Foundry for model data exfiltration attack and track all model data exfiltration for appropriateness and vulnerability/completeness patterns.
- In partnership with external partners, monitor AI tools and environments to ensure models are not exposed and all components are sourced from reputable sources and have robust secure integration.
- Robustly document and review all Agent permissions to ensure the secure deployment and manage of Agents within ONRSR.
- Monitor third party threat detection and hunting applications such as CrowdStrike, Defender and Sentinel alerts. Review and assess Azure Advisor recommendations, applying recommended changes via the CAB.
- Responsible for threat analysis and identification across systems and AI assets
- Responsible for monitoring vulnerability announcements and CVE's for systems, AI and development action, working with IT partners to provide recommendations to mitigate risk, implementing approved actions in a timely manner.
- Responsible for the managing and addressing internal and external audit findings in relation to cyber security posture and infrastructure, appropriately remediating risks identified in a timely manner.
- Ensure that the Data, Infrastructure and Identity pillars of 'Zero Trust' are implemented consistent with the approved architecture including Conditional Access, Least Privilege etc.

	• Ensure policy updates are applied consistently across devices. • Actively review and manage logs including log analytics for critical systems. • Ensure that breach response plans are developed and reviewed and undertake periodic evaluation. Conduct incident reviews as required and produce post-incident reports with lessons learned • Lead containment, eradication, and recovery activities. • In partnership with external vendors to monitor and provide recommendations to adapt ONRSR Threat & Vulnerability framework and controls to ensure alignment to current industry threat vectors and product announcements. • Provide oversight and monitoring of security controls, regularly assessing and evaluating our security posture to provide recommendations to the Manager, Information Security on enhancements that could be made. • Provides support on delivery of IT services, application development and delivery, and enterprise architecture development and deployment.
Key Competencies	Key to success in this role is that you have: • an exceptional understanding of software development and its inherent vulnerabilities • an exceptional understanding of Secure Software development principles • a robust understanding of various software development frameworks • an understanding of AI architectures for Generative, ML and Agentic AI
Qualifications and Experience	Key to success in this role is that you have: • 5+ years' experience in a cyber security role with a software/application security focus. • a Bachelor's degree in cyber security, Computer Science, Information Technology, or a related field. • Microsoft 365 Certified: Security Operations Analyst Associate and/or Microsoft 365 Certified: Azure Security Engineer Associate • Experience working within regulated environments. • Certified Information Systems Security Professional (CISSP) • Secure Software Practitioner (SSCP or CSSLP) • Understanding of Microsoft AI architectures and how to secure them. • CompTIA PenTest+ or similar • Microsoft 365 Certified: Endpoint Administrator Associate • ISACA Advanced in AI Security Management AI & ML Security Certification (e.g. CertNexus Certified AI Practitioner + AI Security) would be advantageous.
Capability Framework	• Cultural Capability Framework (L5-S2, RSO 2,3) • Cyber Security Analyst

Your compliance	As a regulator, it is important that we are all on the same page when it comes to safety and risk management and everyone at ONRSR is responsible for actively supporting this aspect of our role to promote a positive and safe culture. ONRSR has a zero tolerance to the use of alcohol and non-prescription drugs for all workers while undertaking ONRSR work, in accordance with the Drug and Alcohol Policy.
Special Conditions	Special conditions that apply to this role include: • On occasions, this role may require you to work outside of normal business hours, on weekends and public holidays. • There is a requirement to travel which may include short stays in ONRSR interstate offices. • Required to complete a national police check • Hold and maintain the right to work in Australia
Privacy Notification	ONRSR requires personal information and documents relevant to your employment. The collection and handling of this information will be consistent with the requirements of relevant privacy laws.
Our Commitment to You	ONRSR is genuinely committed to investing in the capability of its team and is proud of its structured approach to supporting capability and development of all employees in a supportive environment. All team members are considered regulatory team members whether infield or enabling and can access opportunities to learn key skills in their role and about regulation through a range of programs including our Regulatory Officer Training Program. The success of these programs relies on your engagement, openness to learning and willingness to share with your peers. ONRSR expects its people to contribute to the efficient and effective functioning of the organisation to meet ONRSR and team strategic goals. This includes actively participating in the Performance Development Plan; demonstrating appropriate and professional behaviours in accordance with the Code of Conduct, Respect and Inclusion at ONRSR Policy and Culture Blueprint; providing assistance to team members if required; and undertaking other key responsibilities or activities as directed.
Your Commitment to ONRSR	I have read and understood the requirements of the position and agree to carry out the key responsibilities to the best of my ability. I understand that I may be required to perform other duties from time to time to fulfill the position requirements.

Employee Signature:	Date:
----------------------------	--------------